0172.42240X00
NC 19997 US

FASTER AUTHENTICATION WITH PARALLEL MESSAGE PROCESSING

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of the filing date of Provisional Application Serial No. 60/426,794, filed November 18, 2002, entitled "Faster Authentication With Parallel Message Processing in SeNAA" which application is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

[0002] Explanation of Abbreviations Used

PANA	Protocol for carrying Authentication for Network Access Authentication
PAA	PANA Authentication Agent
PaC	PANA Client
TLS	Transport Level Security
EAP	Extensible Authentication Protocol
AAAH	AAA Home server
MN	Mobile Node
DoS	Denial of Service
SeNAA	Secure Network Access Authentication
LSA	Security Association
AAA	Authentication, Authorization and Accounting

Field of the Invention

[0003] The invention relates to a method and a system for expediting in at least one network the establishment of a secure tunnel which provides connection between user equipment (UE) and one network entity and authenticating the user equipment with another network entity.

Description of the Prior Art

[0004] The IETF draft (draft-forsberg-pana-secure-network-access-auth-00.txt), presents a link layer independent network access authentication method, Secure Network Access Authentication (SeNAA), to support smooth interaction between (UE) and access networks while roaming. The draft authentication method has two phases, I and II. Phase I must be completed before phase II can be started. The serial message processing is slow.

[0005] Fig. 1 depicts the original (draft) version of the authentication protocol which was not adopted. Mobile terminals utilize different link layer technologies and roam between different layers. A generic link layer independent authentication and authorization method is needed to support smooth interaction between UE and access networks while roaming. UE network access authentication in different network technologies has become an important issue in the Internet. Different authentication methods already exist but are more or less link layer dependent.

[0006] SeNAA uses User Datagram Protocol (UDP) as the transport protocol. UDP is a lightweight protocol and allows application level implementations with port numbers. UDP carries DIAMETER formatted SeNAA messages. SeNAA provides

reliable request and response style message delivery (re-transmission and duplicate packet detection).

[0007] SeNAA does not assume a secure channel between PaC and PAA. Thus, on top of the SeNAA protocol TLS, a protocol is used to negotiate a Local Security Association (LSA) between PaC and PAA. TLS provides authentication, privacy, integrity, and replay protection. TLS is used to protect SeNAA message AVPs and EAP between PaC and PAA. AVPs that need protection are fed to the TLS Record layer, and the resulting encrypted and compressed data is stored into a TLS-Payload AVP. EAP protocol is carried inside an EAP-Payload AVP. SeNAA messages after successful TLS handshake are integrity protected with a check sum stored in the Msg-Checksum AVP. The AVP is protected with TLS Record layer.

[0008] TLS is also used for re-authentication between PaC and PAA. TLS supports mutual authentication and can optionally be used instead of EAP for user authentication. In all cases TLS is used for access network authentication. SeNAA messages carry information such as the PaC's Device Identifier (DI), that must be integrity protected. If PAA supports DIAMETER and/or RADIUS AAA back-end, signaling between PaC and PAA can easily be extended to the back-end. SeNAA doesn't rely on any modifications to the EAP protocol. It provides secure transport up to the PAA for EAP. Thus, any existing EAP methods can be used securely with SeNAA between PaC and PAA. Security after PAA is outside the scope of SeNAA. PAA is assumed to get user authentication answer (Success or Failure) from the authenticator.

[0009] SeNAA utilizes protocols like EAP, TLS, UDP and IP that are assumed to exist in the PaC terminal already even without SeNAA. Fig. 2 illustrates an exemplary one. DIAMETER like message formatting and request/response style reliability transport is one additional requirement for the PaC terminal and is provided with the SeNAA protocol. TCP and SCTP are considered too heavy weight transport protocols for SeNAA purposes (i.e. more message round trips needed).

[0010] Data protection, such as IP datagrams, is out of the scope of SeNAA. One possibility for further studies is to use the key material produced in the TLS handshake process with IPSec.

[0011] With reference to Fig. 1, successful mutual authentication is divided into two phases. In Phase I the network is authenticated, and the user is authenticated in Phase II.

[0012] Phase I consists of a TLS handshake as is shown in Fig 3A which provides initial authentication with TLS to provide a secure tunnel. Local re-authentication, where PaC authenticates to PAA, is in Phase I and is handled with TLS Session Resumption (illustrated in Fig. 3B which provides re-authentication with TLS). Access network authentication is based on access network certificates. How certificates are created, processed and verified is known and not described herein.

[0013] Phase II uses EAP for authenticating the user (Fig. 4 illustrates user authentication signalling with EAP being carried inside the EAP-Payload AVP). User authentication is bound to the DI, which is used to control access to the network.

[0014] With reference to Fig. 1, in Phase I, Server-Certificate-Request (SCR) message carries Client-Hello TLS message. Server-Certificate-Answer (SCA) carries

the TLS answer which contains the Access Network certificate. PaC verifies the certificate. PAA also adds a Session-Id AVP into the SCA message. This Session-Id is different from the TLS session-Id. The next messages must have the AVP included during the whole session. To finish the TLS handshake, PaC sends Client-Security-Association-Request (CSAR) message to the PAA. PAA answers with Client-Security-Association-Answer (CSAA).

[0015] When TLS is not used, a different UDP port number (PAA UDP port <UDP-port3>, PaC UDP port <UDP-port4>) must be used for plaintext CLR/CLA message delivery. PaC can decide not to use Phase I authentication but must use Phase I authentication if <UDP-port3> is not reachable. Similarly if UDP port <UDP-port1> is not reachable, PaC should try to use UDP port <UDP-port3>.

[0016] In Phase II, after a successful TLS handshake, PaC uses AAA-Client-Request (CLR) message to start user authentication and DI authorization. CLR carries EAP-Payload AVP to PAA. PAA answers with AAA-Client-Answer (CLA) message with a Result-Code AVP. Result-Code informs PaC if multiple round trips are needed for completing the EAP authentication method or if the authentication (authorization) succeeded or failed.

[0017] PaC adds DI(s) thereof into the CLR message so that PAA can verify the integrity of the DI and optionally provide it for the enforcement point.

[0018] PAA can be co-located in the ARs or separated from the ARs. In case of separation, ARs act as relay agents to PAA for MN. PAA is in the same subnet as the AR and MN. When PAA receives a message from MN through an AR, it must send the reply directly to the MN. When PAA is separated from ARs, an AR should

relay MN's SeNAA messages to the PAA. When MN receives an answer from PAA, the MN must send further requests to the PAA directly.

[0019] SeNAA uses request and response style transactions. For each request a response is sent. If a response is not received in time, the request is re-sent. This mechanism is used for packet loss recovery. The received response works as an acknowledgment. SeNAA uses DIAMETER message formatting. The DIAMETER message header provides packet duplication (End-to-End Id) detection and request/response mapping (Hop-by-Hop Id).

[0020] To protect integrity of the DIAMETER header and the whole message, MAC is calculated over the DIAMETER message. The MAC is put into an AVP called Msg-Checksum. CLR/CLA messages use this AVP. PaC needs to be authenticated before network access is granted through the enforcement point (EP) in the access network.

[0021] Authentication and re-authentication initiator can be PaC or PAA.

[0022] PaC starts re-authentication by sending CSAR message with TLS Client Hello in the TLS-Payload AVP to PAA to UDP port <UDP-port1> (Fig. 3B). Similarly, PAA initiates re-authentication by sending CSAA message with TLS Server Hello message in the TLS-Payload AVP to PaC to UDP port <UDP-port2>. The hello message contains the current TLS session specific id, which is used to detect session resumption from initial authentication. Re-authentication involves multiple CSAR/CSAA round trips.

[0023] After a TLS handshake or session, resumption is done and the SA is established PaC uses the TLS Record Layer to encrypt SeNAA message AVPs.

[0024] SeNAA doesn't assume connection-oriented links. Thus, TLS re-authentication is used for notifying PAA of PaC's presence. Re-authentication interval is implementation specific <TBD?>.

[0025] TLS Alert, Handshake and Change cipher specification protocols are carried inside TLS Record Layer. For example if TLS Alert protocol reports a fatal error it is delivered with the next TLS-Payload AVP or with separate CSAR/CSAA messages. The SeNAA application must understand the return codes from TLS Record Layer API functions. When fatal error is received, the TLS session is torn down. The SeNAA session MUST be re-negotiated.

[0026] TLS message formats can be found from TLS. The DIAMETER message header format and AVP format is known. SCA and CSAA messages do not contain Result-Code AVPs.

[0027] Format of the SCR message:

```
< Server-Certificate-Request > ::= < Diameter Header: <TBD>,
                                   REQ, PXY >
          { User-Name }
          { TLS-payload }
```

TLS-Payload AVP contains the TLS handshake messages in the AVP data area as specified in [TLS]. The TLS-Payload AVP contains TLS-Client-hello.

Format of the SCA message:

```
< Server-Certificate-Answer > ::= < Diameter Header: <TBD>, PXY >
          < Session-Id >
          { TLS-payload }
```

A Session-Id is generated for the PaC and delivered in the Session-Id AVP.

The TLS-Payload AVP contains TLS Server-hello, TLS Server-Certificate, TLS server-Key-Exchange, and TLS Server-Hello-Done messages.

Format of the CSAR message:

```
< Client-Security-Association-Request > ::= < Diameter Header: <TBD>,
                                            REQ >
          < Session-Id >
          { TLS-payload }
```

The Session-Id AVP is used in every SeNAA message between PaC and PAA.

The TLS-Payload contains TLS-Client-Key-Exchange, TLS-Change-Cipher-Spec, and TLS-Client-Finished messages.

[0028] Format of the CSAA message:

< Client-Security-Association-Answer > ::= < Diameter Header: <TBD>, PXY >
< Session-Id >
{ TLS-Payload }

The TLS-Payload contains TLS-Change-Cipher-Spec and TLS-Server-Finished messages.

[0029] Format of the initial CLR message:

< AAA-Client-Request > ::= < Diameter Header: <TBD>, REQ, PXY >
[TLS-Payload:
< Session-Id >
{ User-Name }
{ Device-Identity }
[EAP-Payload]
[Authorization-Lifetime]
[Msg-Checksum]
]

The TLS-Payload AVP data area contains encrypted AVPs through TLS Record layer.

[0030] Format of the CLA message from PAA to PaC:

< AAA-Client-Answer > ::= < Diameter Header: <TBD>, PXY >
[TLS-Payload:
< Session-Id >
{ Result-Code }
[EAP-payload]
[Authorization-Lifetime]
[Auth-Grace-Period]
[Multi-Round-Time-Out]
[Msg-Checksum]
]

The TLS-Payload AVP data area contains encrypted AVPs through TLS Record layer.

[0031] The TLS-Payload AVP data contains encapsulated AVPs that are encrypted and compressed by TLS Record layer. Upon receive of TLS-Payload AVP the data area is first fed to the TLS Record layer to get the plain text AVP list for further processing.

[0032] The Msg-Checksum AVP data contains checksum of the whole DIAMETER message. Msg-Checksum is calculated over the message with Msg-Checksum AVP data area bits set to zero. Checksum algorithm is <TBD>.

[0033] The CLA message contains TLS protected Result-Code AVP. In SeNAA one of the following Result-Code values is possible.

DIAMETER_MULTI_ROUND_AUTH 1001
EAP user authentication requires more round trips.
DIAMETER_SUCCESS 2001
EAP user authentication and network access authorization successful.
DIAMETER_AUTHENTICATION_REJECTED 4001
EAP user authentication failure.

[0034] SeNAA provides reliable request and response style transactions. Peer which initiates the transaction is responsible for re-transmission if the corresponding response is not received in <TBD-msec1> milliseconds. Maximum number of retries is <TBD-retries1>.

[0035] If Multi-Round-Time-Out AVP is included in a SeNAA message from PAA to PaC, the re-transmission (same Hop-by-Hop Id and End-to-End Id) MUST not exceed this time limit.

[0036] UDP Port number(s) must be defined. SCR/SCA, CSAR/CSAA and CLR/CLA message command codes must be assigned. Msg-Checksum and TLS-Payload AVP codes must be assigned.

[0037] Fig. 1 as described above illustrates the use of DIAMETER-EAP authentication. In the first step, the EAP client is requested to initiate the authentication procedure. Normally, the client (EAP peer) authentication is requested by the EAP authenticator or an access point, but one round-trip of EAP messages is saved when the client device, which comprises the EAP client, initiates the authentication request (EAP Request (Identity)). The EAP client responds to the request and provides an identity in the response message.

[0038] In the next step, the client or UE request the server in the access network (access router) to authenticate itself. The client sends a message (client hello in this embodiment where TLS is used) to the server, the message containing a session ID and information on the client's supported cryptographic algorithms. The client can indicate in the message, from which certifying authority it wishes the server to acquire its security certificate. The server responds with a server hello message, indicating the selected encryption/validation algorithm, as well as provides a security certificate to the client. The next messages conclude Phase I, establishing a secure connection between the client and the server in the access network. Both the client and the server send a finished message to confirm that the key exchange and authentication were successful.

[0039] In Phase II, the client authentication stage, uses the secure connection established between the client and the server for exchanging authentication information with an authentication server. The client sends an authentication request, which is to be passed on to the authenticator by the access point server. The message contains, for example, the client ID which the client received from the EAP

peer in the first step. The server in the access network forwards the authentication request to the AAA home server, which in turn forwards the EAP response (received from the EAP peer/client in step 1) to the EAP authenticator. In the next step, the EAP authenticator indicates that it is not satisfied with the client's identity information only, but requires an additional authentication round. The EAP authenticator sends an EAP request toward the client with a 'multi-round' result code, which indicates, that an additional round trip is required for authentication. The EAP authenticator indicates in the EAP request sent toward the client, which type of further authentication is requested from the client. The message is then forwarded through the AAA infrastructure to the EAP client, which creates the required response to the authentication request and sends the response back toward the EAP authenticator through the AAA infrastructure. When the EAP authenticator receives the client's response, it checks whether the response was as expected, and in case of a valid response, the EAP sends a message indicating successful authentication toward the client.

[0040] Fig. 5 illustrates a prior art diagram of a generic system and process in which serial processing involving phases I and II, like Fig. 1, is illustrated between UE, an access network and a home network which may be an AAA home network. Phase I represents the establishment of a secure tunnel between the UE and the access network and Phase II represents authentication of the UE with the home network. As may be seen, the establishment of a secure connection (Phase I) precedes the authentication of the UE (Phase II) in the home network. This serial process has the resultant time delay.

[0041] Fig. 6 illustrates a prior art diagram of a generic system and process in which serial processing involving Phases I and II, like Figs. 1 and , is illustrated between a UE and one of either a home network or a visited network network. Like the processing described above in conjunction with Figs. 1 and 5, the processing is serial involving Phases I and II with the attendant time delay. A single network entity in the home or visited network is the point of exchange with the Request and Answer messages involving Phases I and II.

[0042] First, the UE or client requests the access network server to authenticate itself, the server provides the client with its security certificate, and the key exchange and authentication is confirmed by "finished" messages sent by both the client and the server. The client sends an authentication request through the network infrastructure which may be an AAA architecture toward the authentication server, the authentication server challenges the UE to provide additional authentication information, and once the server receives a valid response to its challenge from the UE, the server sends a message indicating successful authentication toward the UE through the infrastructure.

SUMMARY OF THE INVENTION

[0043] The present invention is a method and a communication system for connecting a client or UE to at least one network including network entities. With the invention, authenticating the client or UE with one network entity occurs at least partially simultaneously (partially in parallel) with the establishing of a secure tunnel. The authentication of the UE may start at the same time as the establishing of the

secure tunnel or thereafter to be only partially simultaneous therewith. This methodology provides time savings.

[0044] The present invention in first and second embodiments combines authentication phases I (TLS) and II (EAP Over DIAMETER) with parallel message processing to obtain a faster authentication process in SeNAA. In one embodiment with maximum overlap, a possibility of an easy DoS attack against AAAH exists. In another embodiment, with less than totally simultaneous processing when a DoS attack is detected, the level of vulnerability to the DoS attack is decreased. The embodiment with maximum overlap of Phase I and II is the fastest solution, but the other embodiment with partial overlap is still faster than the prior art draft version illustrated in Fig. 1 and provides protection against DoS.

[0045] Moreover, when the overlap between the establishing of the secure tunnel and the authenticating of the UE is partial, with the establishing of the secure tunnel being established first, at least one network communicates with the UE to confirm that the request from the UE for a secure tunnel is not part of a DoS attack. The communication during the overlap time may include at least one of a request for an identification of the UE and a request for capability of the UE to support at least one data protocol.

[0046] A used herein a network entity may be a physical or logical entity, such as without limitation, a server.

[0047] As used herein, the home network is the network with billing responsibility for the UE.

[0048] In a communication system comprising at least one network, including network entities which provide connectivity to user equipment, a method of connecting the user equipment to the at least one network in accordance with the invention includes establishing a secure tunnel which provides connection between the user equipment and one of the network entities; and authenticating the user equipment with another of the network entities; and wherein the authenticating of the user equipment with the another of the network entities occurs at least partially simultaneously with the establishing of the secure tunnel. The establishing the secure tunnel and the authenticating the user equipment with the network may begin simultaneously or begin before the authenticating the user equipment with the network. During a time between a beginning of the establishing the secure tunnel with the one of the network entities and a beginning of the authenticating the user equipment with the another of the network entities, the at least one network may communicate with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack. The communication during the time may include at least one of a request for an identification of the user equipment and a request for capability of the user equipment to support at least one data protocol. The one network entity may comprise a server and the another network entity may comprise a server. In an access network which provides connection of the user equipment to the network, the secure tunnel may be established between the user equipment and the access network and the one network entity may be part of the access network. The user equipment may be wirelessly connected to the at least one network. The at least

one network may comprise an access network and a home network, or a visited network

[0049] A communication system in accordance with the invention includes at least one network, including network entities which provide connectivity to user equipment and wherein a secure tunnel is established which provides connection between the user equipment and one of the network entities, the user equipment is authenticated with another of the network entities, and the authenticating of the user equipment with the another of the network entities occurs at least partially simultaneously with the establishing of the secure tunnel. The establishing the secure tunnel and the authenticating the user equipment with the network may begin simultaneously or begin before the authenticating the user equipment with the network. During a time between a beginning of the establishing the secure tunnel with the one of the network entities and a beginning of the authenticating the user equipment with the another of the network entities, the at least one network may communicate with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack. The communication during the time may include at least one of a request for an identification of the user equipment and a request for capability of the user equipment to support at least one data protocol. The one network entity may comprise a server and the another network entity may comprise a server. In an access network which provides connection of the user equipment to the network, the secure tunnel may be established between the user equipment and the access network and the one network entity may be part of the access network. The user equipment may be wirelessly connected to the at

least one network. The at least one network may comprise an access network and a home network, or a visited network

[0050] The invention further is a user equipment in a communication system comprising at least one network, including network entities which provide connectivity to the user equipment and wherein: a secure tunnel is established which provides connection between the user equipment and one of the network entities, the user equipment is authenticated with another of the network entities, and the authenticating of the user equipment with the another of the network entities occurs at least partially simultaneously with the establishing of the secure tunnel. The establishing the secure tunnel and the authenticating the user equipment with the network may begin simultaneously before the authenticating the user equipment with the network. During a time between a beginning of the establishing the secure tunnel with the one of the network entities and a beginning of the authenticating the user equipment with the another of the network entities, the at least one network may communicate with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack. Communication during the time may include at least one of a request for an identification of the user equipment and a request for capability of the user equipment to support at least one data protocol. The one network entity may comprise a server and the another network entity comprises a server. An access network may provide connection of the user equipment to the network and the secure tunnel may be established between the user equipment and the access network and the one network entity may be part of the access network. The user

equipment may wirelessly be connected to the at least one network. The access network may communicate with the user equipment to confirm
that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack.

BRIEF DESCRIPTION OF THE DRAWINGS

[0051] Fig. 1 illustrates the prior art serial establishment of a secure tunnel and authenticating a client using a DIAMETER-EAP authentication.

[0052] Fig. 2 illustrates the prior art SeNAA protocol stack in PaC.

[0053] Fig. 3A illustrates the prior art initial authentication of Fig. 1 with TLS.

[0054] Fig. 3B illustrates the prior art re-authentication of Fig. 1 with TLS.

[0055] Fig. 4 illustrates user authentication signalling of Fig. 1 with EAP being carried inside EAP-Payload AVP.

[0056] Fig. 5 illustrates a generic prior art diagram of serial establishment of a secure tunnel and authentication of UE in a system including a UE, an access network and a home network which may be an AAA network.

[0057] Fig. 6 illustrates a generic prior art diagram of serial establishment of a secure tunnel and authentication of a UE in a system including UE and one of a home network or visited network.

[0058] Figs. 7 and 8 illustrate first and second embodiments of the invention which improve the prior art serial processing of Fig. 1 by providing for at least some simultaneous processing of the establishment of the secure tunnel and authentication of the user.

[0059] Figs. 9 and 10 illustrate third and fourth embodiments of the invention which improve the prior art processing of Fig. 5 by providing for at least some simultaneous processing of the establishment of the secure tunnel and authentication of the user.

[0060] Figs. 11 and 12 illustrate fifth and sixth embodiments of the invention which improve the prior processing of Fig. 6 by providing for at least some simultaneous processing of the establishment of the secure tunnel and authentication of the user.

[0061] Figs. 13-18 respectively illustrate the modification of the embodiments of Figs. 7-12 to include protection against DoS attacks.

[0062] Like parts or signal flows are identified identically throughout the drawings.

DESCRIPTION OF THE PREFERRED EMBODIMENTS OF THE INVENTION

[0063] Figs. 7 and 8 illustrate first and second embodiments of the invention which improve the speed of establishing a secure tunnel and authentication of the user by using at least partial simultaneous processing of the establishment of the secure tunnel (Phase I) and the establishment of authentication of the user (Phase II) when compared to the prior art of Fig. 1. The specific signal flows that are separately illustrated as parts of Phases I and II, may be combined into a single message where possible. The individual signal flows are identical to the prior art of Fig. 1 and are not hereafter described. The first embodiment of Fig. 7 has a greater degree of signal processing overlap than the second embodiment of Fig. 8. Fig. 7 depicts an optimized parallel message processing solution for the prior art of Fig. 1

with maximum overlap. Fig. 8 depicts the optimized solution, when a DoS attack against AAAH has been detected with less than maximum overlap to permit return signalling to the UE to request an identification of the UE, a request of the capability of the UE or other prior art signalling to determine if a DoS attack is occurring.

[0064] Figs. 9 and 10 illustrate third and fourth embodiments of the invention which improve the speed of establishing a secure tunnel and authentication of the user by using at least partial simultaneous processing of the establishment of the secure tunnel (Phase I) and the establishment of the authentication of the user (Phase ii) when compared to the prior art of Fig. 5. The specific signal flows, that are separately illustrated as parts of Phases I and II, may be combined into a single message where possible. The individual signal flows are identical to the prior art of Fig. 5 and are not hereafter described. The embodiment of Fig. 10 has a greater degree of signal processing overlap than the embodiment of Fig. 9.

[0065] Figs. 11 and 12 illustrate fifth and sixth embodiments of the invention which improve the speed of establishing a secure tunnel and authentication of the user by using at least partial simultaneous processing of the establishment of the secure tunnel (Phase I) and the establishment of the authentication of the user (Phase II) when compared to the prior art of Fig. 6. The specific signal flows, that are separately illustrated as parts of Phases I and II, may be combined into a single message where possible. The individual signal flows are identical to the prior art of Fig. 6 and are not hereafter described. The embodiment of Fig. 12 has a greater degree of signal processing overlap than the embodiment of Fig. 11.

[0066] Each of the home and/or visited networks of the six embodiments of the invention include separate network entities (not illustrated) within the home and/or visited network at which the establishment of the secure tunnel and authentication of the user are terminated.

[0067] The embodiments of Figs. 13-18 represent the modification respectively of the embodiments of Figs. 7-12 to mitigate against DoS attack vulnerability during the authentication phase (Phase I) involving the client or UE computing and storing state information. Figs. 13-18 respectively modify the embodiments of Figs. 7-12 to include a DoS Inquiry and a Response to DoS Inquiry to provide protection against DoS attacks. If the second phase (Phase II) is started at the same time as the first phase (Phase I), namely at the occurrence of the first message from the client or UE to the network, the network elements that are involved with the second phase authentication are more easily involved with DoS signalling. Dynamic DoS attack prevention is used to protect the network entities involved in the second phase from malicious users providing flooding packets. The method for doing this is to start the second phase later and later depending on the malicious packet signalling. This makes the DoS attack against the second phase network entity harder, because the malicious client or UE has to do more in the first phase before second phase is started. Ultimately, the system can fall back to the state, where Phase I is completely finished before the second phase starts, as in the prior art of Figs. 1, 5 and 6. It should be noted that the invention is not limited to the timing of the DoS inquiry and the Response to DoS inquiry as illustrated relative to Phases I and II.

[0068] How to detect DoS attacks is not part of the present invention since detection thereof is well known. The at least one network can, for example, detect the number and the time interval of the initial authentication messages and base the decision thereon to fall back to the serialized processing mode of the prior art to avoid the DoS attack.

[0069] Depending on the first phase authentication signalling system, Phase II can be started in different phases of the Phase I authentication (as in Figs. 7-12). How to combine the phases depends on the protocols and authentication methods.

[0070] Also privacy may be a concern addressed by the present invention if the second phase includes information that needs to be protected with the first phase. However, the second phase signalling can start without protection and continue with protection when first phase is finished.

[0071] While the invention has been described in terms of its preferred embodiments, it should be understood that numerous modifications may be made thereto. It is intended that all such modifications fall within the scope of the appended claims.